



Posudek vedoucího bakalářské práce

| | |
|-----------------|---|
| Jméno studenta: | Farkas Marek |
| Téma práce: | Dostupné zdroje entropie a jejich kvalita v systémech Linux a Windows |
| Cíle práce: | <p>Budou vysvětleny pojmy týkající se entropie, hustoty informací a náhodnosti. Budou popsány známé metodiky hodnocení kvality generátorů náhodných čísel.</p> <p>Bude zváženo a posouzeno co možná největší počet možných zdrojů entropie dostupných na osobních počítačích využitelných v operačních systémech Linux a Windows. Posouzeny budou jak možné hardwarové, tak i softwarové zdroje entropie. Každý zdroj bude posouzen z hlediska kvality generovaných číselných posloupností se zaměřením na jeho praktické využití v kryptografii. Zváženy budou i nehodící se zdroje, které trpí závažnými nedostatky, jež budou popsány.</p> |

Náročnost zadání bakalářské práce na:

- teoretické znalosti: vyšší,
- praktické zkušenosti: střední,
- podkladové materiály (vstupní data) a jejich zpracování: vyšší.

A. Slovní hodnocení:

| |
|--|
| Naplnění cíle práce: |
| Všechny cíle byly splněny. |
| Logická stavba a stylistická úroveň práce: |
| Text je logicky členěn do navazujících kapitol, stylisticky v pořádku. |
| Využití záměrů, námětů a návrhů v praxi: |
| Lze využít zejména pro generování klíčů určených pro šifrování. |
| Případné další hodnocení (připomínky k práci): |
| – |

B. Kriteriaální hodnocení:

| Kritéria hodnocení práce | Úroveň | Připomínky |
|--|-------------|-------------------------------------|
| Úroveň dokumentu | | |
| logická stavba práce | nadprůměrné | |
| stylistická úroveň | průměrné | |
| práce s literaturou včetně citací | nadprůměrné | |
| formální úprava práce (text, grafy, tabulky) | průměrné | Nalezeno několik pravopisných chyb. |
| Teoretická část | | |

| Kritéria hodnocení práce | Úroveň | Připomínky |
|---|--------------------------|------------|
| rozsah a úroveň zpracování řešerše | nadprůměrné | |
| formulace teoretických východisek pro praktickou část | nelze hodnotit | |
| odborné zvládnutí problematiky | nadprůměrné | |
| Praktická část – produkt (řešení) | | |
| adekvátnost použitých metod, SW, postupů | průměrné | |
| kvalita návrhu řešení | nelze hodnotit | |
| komplexnost řešení | nelze hodnotit | |
| návrh datových struktur | nelze hodnotit | |
| uživatelské rozhraní | nelze hodnotit | |
| odborné zvládnutí problematiky | nadprůměrné | |
| rozpracovanost | dokončeno, otestováno | |
| využitelnost praktické části v praxi | ve větší míře | |
| Praktická část – popis | | |
| popis řešení v bakalářské práci | nadprůměrné | |
| ostatní přílohy (tabulky, grafy, výpočty, ...) | nadprůměrné | |
| uživatelská příručka | nelze hodnotit | |
| Uložení dokumentu/ů bakalářské práce na CD | ano | |
| Uložení výsledku praktické části na CD | ano | |
| Stupeň splnění cíle práce | splněn | |

C. Otázky k obhajobě (max. 2):

1. Konzultoval jste s externím vedoucím využitelnost vámi popsaných metod v praxi? Budou výsledky nějak využity?
2. Plánujete do budoucna podrobnější výzkum zdrojů entropie s detailnějším ověřováním zejména po teoretické stránce?

Doporučení k obhajobě: ano

Navržený klasifikační stupeň: výborně

Posudek vypracoval(a):

Jméno, tituly: Mgr. Tomáš Hudec

Zaměstnavatel: UPa, FEI, KIT

V Pardubicích dne 29. 5. 2014

Podpis: